

明 細 書

情報管理装置及び情報管理方法

技術分野

- [0001] 本発明は、比較的大容量のメモリ領域に格納された情報へのアクセスを管理する情報管理装置及び情報管理方法に係り、特に、メモリ領域上に電子的な価値情報を格納して電子決済を始めとするセキュアな情報のやり取りを行なう情報管理装置及び情報管理方法に関する。
- [0002] さらに詳しくは、本発明は、メモリ領域上にさまざまなファイルを割り当てて、サービス運用のための情報を管理する情報管理装置及び情報管理方法に係り、特に、メモリ領域上に電子的に格納されている価値情報のコピー若しくはバックアップを行ない、端末間での価値情報の移動を円滑に行なう情報管理装置及び情報管理方法に関する。

背景技術

- [0003] ICカードに代表される非接触・近接通信システムは、操作上の手軽さから、広範に普及している。ICカードの一般的な使用法は、利用者がICカードをカード・リーダ／ライタをかざすことによって行なわれる。カード・リーダ／ライタ側では常にICカードをポーリングしており外部のICカードを発見することにより、両者間の通信動作が開始する。例えば、暗証コードやその他の個人認証情報、電子チケットなどの価値情報などをICカードに格納しておくことにより、キャッシュ・ディスペンサやコンサート会場の出入口、駅の改札口などにおいて、入場者や乗車者の認証処理を行なうことができる。
- [0004] 最近では、微細化技術の向上とも相俟って、比較的大容量のメモリを持つICカードが出現している。大容量メモリ付きのICカードによれば、メモリ空間上にファイル・システムを展開し、複数のアプリケーションを同時に格納しておくことにより、1枚のICカードを複数の用途に利用することができる。例えば、1枚のICカード上に、電子決済を行なうための電子マネーや、特定のコンサート会場に入場するための電子チケットなど、複数のアプリケーションを格納しておくことにより、1枚のICカードをさまざまな用

途に適用させることができる。ここで言う電子マネーや電子チケットは、利用者が提供する資金に応じて発行される電子データを通じて決済(電子決済)される仕組み、又はこのような電子データ自体を指す。

[0005] また、ICカードやカード用リーダ／ライタ(カード読み書き装置)が無線・非接触インターフェースの他に、外部機器と接続するための有線インターフェースを備え、携帯電話機、PDA(Personal Digital Assistance)やCE(Consumer Electronics)機器、パーソナル・コンピュータなどの各機器に内蔵して用いることにより、これらの機器にICカード及びカード・リーダ／ライタのいずれか一方又は双方の機能を装備することができる。このような場合、ICカード技術を汎用性のある双方向の近接通信インターフェースとして利用することができる。

[0006] 例えば、コンピュータや情報家電機器のような機器同士で近接通信システムが構成される場合には、ICカードを利用した非接触通信は一対一で行なわれる。また、ある機器が非接触ICカードのような機器以外の相手デバイスと通信することも可能であり、この場合においては、1つの機器と複数のカードにおける一対多の通信を行なうアプリケーションも考えられる。

[0007] また、電子決済を始めとする外部との電子的な価値情報のやり取りなど、ICカードを利用したさまざまなアプリケーションを、情報処理端末上で実行することができる。例えば、情報処理端末上のキーボードやディスプレイなどのユーザ・インターフェースを用いてICカードに対するユーザ・インタラクションを情報処理端末上で行なうことができる。また、ICカードが携帯電話機と接続されていることにより、ICカード内に記憶された内容を電話網経由でやり取りすることもできる。さらに、携帯電話機からインターネット接続して利用代金をICカードで支払うことができる。

[0008] あるサービス提供元事業者用のファイル・システムをICカードの内蔵メモリに割り当てて、このファイル・システム内で当該事業者によるサービス運用のための情報(例えば、ユーザの識別・認証情報や残りの価値情報、使用履歴(ログ)など)を管理することにより、従来のプリペイド・カードや店舗毎のサービス・カードに置き換わる、非接触・近接通信を基調とした有用なサービスを実現することができる。

[0009] 従来、サービス提供元事業者毎にICカードが個別に発行され、ユーザの利用に供

されていた。このため、ユーザは、利用したいサービス毎にICカードを取り揃え、携帯しなければならなかった。これに対し、比較的大容量のメモリ空間を持つICカードによれば、単一のICカードの内蔵メモリに複数のサービスに関する情報を記録するだけの十分な容量を確保することができる(例えば、非特許文献1を参照のこと)。

- [0010] ICカード内のメモリ領域は、初期状態ではICカード発行者がメモリ領域全体を管理しているが、ICカード発行者以外のサービス提供元事業者がメモリ領域から新たなファイル・システムを分割し、それぞれのサービス運用を実現するためのアプリケーションに割り当てる。ファイル・システムの分割は、仮想的なICカードの発行である。また、メモリ領域の分割操作を繰り返すことにより、ICカード内のメモリ領域は複数のファイル・システムが共存する構造となり、1枚のICカードでマルチアプリケーションすなわち多種多様なアプリケーションを提供することができる。
- [0011] ICカード若しくはICチップ上には、電子マネーや電子チケットといったさまざまな価値情報を安全に格納することができる。利用者の利便性を考慮すると、ICカードに担持されているデータのバックアップをとることが必要となってくる。価値情報を格納したICチップを内蔵した携帯電話機を機種変更する場合や、ICチップを搭載したカードや機器に障害が発生した場合などである。
- [0012] ところが、ICカード内のデータのコピー若しくはバックアップをとる際には、2重化を防止しなければならない。現金の移動であれば、財布から財布へ移動することはあっても、増えることはない。これに対し、電子マネーや電子チケットなどの価値情報は、現金相当の価値を有するものの、その実体はデジタル・データなので、データ移動元のICカードとデータ移動先のICカードの双方に元の価値情報が2重化して存在してしまい、双方で価値情報が利用可能になる可能性がある。
- [0013] また、ICカード内のデータのコピー若しくはバックアップをとる際、正しい相手に移動しなければならない。この際、ICカードがマルチアプリケーション、すなわち複数のサービス提供元事業者の管理下にまたがっている場合には、手続きが煩雑となる。
- [0014] 例えば、携帯電話機の機種変更手続きに併せて、ICチップ内の価値情報を移動することも考えられる。しかしながら、移動途中における通信障害やマシン障害などによる価値情報の消失や、価値情報の不法な複製や改竄が行なわれる可能性があり、

電話会社にとっては責任が過大である。

- [0015] 一方、ICチップ内の各価値情報の移動をそれぞれのサービス提供元事業者によって行なうという方法も考えられる。この方法は責任分離という観点からは有効であるが、ユーザは携帯端末の機種変更に伴い、複数の手続を取らなければならない。
- [0016] 非特許文献1:「無線ICタグのすべて ゴマ粒チップでビジネスが変わる」(106～107頁、RFIDテクノロジー編集部、日経BP社、2004年4月20日発行)

発明の開示

発明が解決しようとする課題

- [0017] 本発明の主な目的は、メモリ領域上にさまざまなファイルを割り当てて、サービス運用のための情報を管理することができる、優れた情報管理装置及び情報管理方法を提供することにある。
- [0018] 本発明のさらなる目的は、メモリ領域上に電子的に格納されている価値情報のコピー若しくはバックアップを行ない、端末間での価値情報の移動を円滑に行なうことができる、優れた情報管理装置及び情報管理方法を提供することにある。

課題を解決するための手段

- [0019] 本発明は、上記課題を参酌してなされたものであり、無線又は有線伝送路を介してデータを送受信する通信部と、前記通信部で送受信するデータを処理するデータ処理部と、前記データ処理部により処理されたファイルを配置するメモリ空間と、バックアップする1以上のファイルについてのアーカイブ・ファイルを、該アーカイブ・ファイルの展開先の識別情報を付して作成するアーカイブ・ファイル作成手段と、を具備することを特徴とする情報管理装置である。
- [0020] ここで言う情報管理装置は、無線通信部及び、データ送受信機能とデータ処理部を有するICチップを内蔵する非接触ICカード、表面に端子を有する接触ICカード、接触／非接触ICカードと同様の機能を有するICチップを携帯電話機、PHS(Personal Handyphone System)、PDA(Personal Digital Assistance)などの情報通信端末装置に内蔵した装置である。また、非接触ICカード機能を搭載したICチップは、RFアナログ・フロントエンドとロジック回路(プロトコル制御、RF変復調、コマンド

処理、暗号処理、メモリ管理)を1チップで構成してもよいし、あるいはこれらを分離した2チップ以上のICで構成するようにしてもよい。以下では、これらを総称して、単に「ICカード」と呼ぶこともある。

- [0021] 本発明に係る情報管理装置は、EEPROMなどのデータ蓄積メモリを含むメモリ領域とデータ処理部を有するとともに、データ通信機能を有するものである。携帯電話機などの場合は、ICチップを内蔵するICカードなどの外部記憶媒体を着脱可能に構成してもよい。また、携帯電話会社が発行する契約者情報を記録したSIM (Subscriber Identity Module) 機能をICチップに搭載してもよい。情報管理装置は、インターネットなどの情報通信ネットワークを介してデータ通信を行なってもよいし、外部端末装置と有線又は無線で直接データ通信を行なってもよい。
- [0022] 本発明は、ICカードが持つ耐タンパ性と認証機能を利用した、価値情報のやり取りなどを含んだセキュリティが要求されるサービスの提供に関するものである。ICカード内のメモリは、一般に、複数のエリアに分割され、エリア毎に異なる暗号鍵を設けてアクセスの制御が行なわれる。ここで言うエリアは、メモリ空間を分割して得られるファイル・システム、若しくはファイル・システム内のディレクトリや個別のファイルに相当する。
- [0023] ここで、利用者の利便性を考慮すると、ICカードに担持されているデータのバックアップをとることが必要となってくるが、特にマルチアプリケーション用途のICカードでは、その処理が煩雑になるという問題がある。
- [0024] これに対し、本発明では、ICカード内のデータから移動先の端末IDを含めたアーカイブ・ファイルを作成し、所定の保管場所に保管するので、価値情報を安全にバックアップすることができる。また、アーカイブ・ファイルは、端末IDで指定された機器でしか展開できないようにする。
- [0025] また、ICカード内のファイルやディレクトリへのアクセスをカウンタで管理する仕組みを導入し、アーカイブ・ファイルを保管場所にアーカイブした後は元のファイルのカウンタ値を消滅させてアクセスできないようにすることで、ファイルの移動を実現することができる。
- [0026] 本発明に係る情報管理装置は、同時にオープンすべきファイルを連携指定するフ

ファイル連携指定手段をさらに備え、アーカイブ・ファイルを作成したファイルと、該ファイルへのアクセス管理情報を記述したアクセス管理情報ファイルとを前記ファイル連携指定手段により連携指定する。そして、前記アクセス管理手段は、アーカイブ・ファイルを作成したファイルへのアクセスが行なわれた際に、アクセス管理情報ファイルを同時にオープンし、アクセス管理情報に基づいてアクセス管理を行なうとともに、アクセス管理情報の内容を更新するようにする。ここで、前記アクセス管理情報ファイルは、アクセス管理情報としてアーカイブ・ファイルを作成したファイルへのカウンタ値を記述しており、前記アクセス管理手段は、アクセス管理情報ファイルをオープンする度にカウンタ値をデクリメントする。

発明の効果

- [0027] 本発明によれば、メモリ領域上にさまざまなファイルを割り当てて、サービス運用のための情報を管理することができる、優れた情報管理装置及び情報管理方法を提供することができる。
- [0028] また、本発明によれば、メモリ領域上に電子的に格納されている価値情報のコピー若しくはバックアップを行ない、端末間での価値情報の移動を円滑に行なうことができる、優れた情報管理装置及び情報管理方法を提供することができる。
- [0029] 本発明のさらに他の目的、特徴や利点は、後述する本発明の実施形態や添付する図面に基づくより詳細な説明によって明らかになるであろう。

図面の簡単な説明

- [0030] [図1]図1は、本発明を適用可能な非接触ICカード通信システムの構成を模式的に示した図である。
- [図2]図2は、ICカードを用いて実現される、電子マネーや電子チケット、その他の価値情報を運用するサービス提供システムの全体的構成を模式的に示した図である。
- [図3]図3は、元のカード発行者が自らのファイル・システムのみを管理しているメモリ領域の状態を示した図である。
- [図4]図4は、カード発行者が自らのファイル・システムの空き領域の内、ある範囲のメモリを領域管理者に貸与(又は譲渡)することが許可できることを示した図である。
- [図5]図5は、他のサービス提供元事業者が、カード発行者から許可された領域にお

いてメモリ領域を分割し、新たなファイル・システムを生成した状態を示した図である。

[図6]図6は、共通領域管理者が、カード発行者から許可された領域において、共通領域のシステム・コードSC0でメモリを分割した状態を示した図である。

[図7]図7は、ICカードのメモリ領域内に複数のファイル・システムが共存する構造を示した図である。

[図8]図8は、ファイル・システム内のデータ構造例を模式的に示した図である。

[図9]図9は、ファイル・システムの基本構成を示した図である。

[図10]図10は、ICカードのメモリ空間においてエリアが階層化されている様子を示した図である。

[図11]図11は、ICカード内のファームウェアの機能構成を模式的に示した図である。

[図12]図12は、ICカード内のファイルやディレクトリをアーカイブするための仕組みを示した図である。

[図13]図13は、ファイルの連携指定したファイル・システム内の基本構成を模式的に示し

[図14]図14は、ディレクトリ内のファイル、あるいはディレクトリとカウンタ・ファイルを連携させているファイル・システム内の構成を模式的に示した図である。

[図15]図15は、本発明の一実施形態に係るICカードのハードウェア構成を模式的に示した図である。

[図16]図16は、ファイル・システム内でファイルの連携関係を設定するための処理手順を示したフローチャートである。

[図17]図17は、ファイル・システム内でファイル連携関係が指定されたファイルに対してアクセスするための処理手順を示したフローチャートである。

符号の説明

- [0031] 1…カード・リーダ／ライタ
2…ICカード
3…コントローラ
111…発行者用通信装置
112…運用者用通信装置

113…製造者用通信装置
114…記憶領域分割登録装置
115…運用ファイル登録装置
116…ICカード
117…ネットワーク
121…カード発行者
122…カード記憶領域運用者
123…装置製造者
124…カード記憶領域使用者
1001…アンテナ部
1002…アナログ部
1003…デジタル制御部
1004…メモリ
1005…外部インターフェース
1006…搬送波検出器
1100…携帯端末
1110…プログラム制御部
1120…表示部
1130…ユーザ入力部
1140…電源制御部

発明を実施するための最良の形態

[0032] 以下、図面を参照しながら本発明の実施形態について詳解する。

[0033] A. ICカードによる非接触データ通信システム

図1には、本発明を適用可能な非接触ICカード通信システムの構成を模式的に示している。

[0034] この非接触カードシステムは、カード・リーダ／ライタ1と、ICカード2と、コントローラ3で構成され、カード・リーダ／ライタ1とICカード2との間では、電磁波を利用して非接触で、データの送受信が行なわれる。すなわち、カード・リーダ／ライタ1がICカー

ド2に所定のコマンドを送信し、ICカード2は受信したコマンドに対応する処理を行なう。そして、ICカード2は、その処理結果に対応する応答データをカード・リーダ／ライタ1に送信する。

[0035] カード・リーダ／ライタ1は、所定のインターフェース(例えば、RS-485Aの規格などに準拠したもの)を介してコントローラ3に接続されている。コントローラ3は、カード・リーダ／ライタ1に対し制御信号を供給することで、所定の処理を行なわせる。

[0036] B. ICカードの運用

図2には、ICカードを用いて実現される、電子マネーや電子チケット、その他の価値情報を運用するサービス提供システムの全体的構成を模式的に示している。

[0037] 図示のシステム100は、例えば、ICカード発行者121が使用する発行者用通信装置111と、カード記憶領域運用者122が使用する運用者用通信装置112と、装置製造者123が使用する製造者用通信装置113と、カード記憶領域使用者124が使用する記憶領域分割装置114及び運用ファイル登録装置115とで構成される。

[0038] ICカード発行者121がカード所有者126にICカード116を発行した場合に、所定の条件に基づいて、カード記憶領域使用者124によって提供されるサービスに係わるファイル・データをICカード116に登録し、カード所有者126が単体のICカード116を用いて、ICカード発行者121及びカード記憶領域使用者124の双方のサービスを受けることを可能にするものである。

[0039] 図2に示すように、システム100では、発行者用通信装置111、運用者用通信装置112、製造者用通信装置113、記憶領域分割装置114及び運用ファイル登録装置115が、ネットワーク117を介して接続される。

[0040] ICカード発行者121は、ICカード116の発行を行なう者であり、ICカード116を用いて自らのサービスを提供する。

[0041] カード記憶領域運用者122は、ICカード発行者121からの依頼を受けて、ICカード発行者121が発行したICカード116内の記憶部(半導体メモリ)に構成される記憶領域のうち、ICカード発行者121が使用しない記憶領域をカード記憶領域使用者124に貸し出すサービスを行なう者である。

[0042] 装置製造者123は、カード記憶領域運用者122から依頼を受けて、記憶領域分割

装置114を製造し、カード記憶領域使用者124に納品する者である。

- [0043] カード記憶領域使用者124は、カード記憶領域運用者122に依頼を行ない、ICカード116の記憶領域を使用して自らの独自のサービスを提供する者であり、メモリ領域を分割して新たなファイル・システムを作成するサービス提供元事業者に相当し、自己のファイル・システムを利用して自身のサービス提供を行なう。
- [0044] カード所有者126は、ICカード発行者121からICカード116の発行を受け、ICカード発行者121が提供するサービスを受ける者すなわちエンドユーザである。カード所有者126は、ICカード116の発行後に、カード記憶領域使用者124が提供するサービスを受けることを希望する場合には、記憶領域分割装置114及び運用ファイル登録装置115を用いて、カード記憶領域使用者124のサービスに係わるファイル・データをICカード116に記憶し、その後、カード記憶領域使用者124のサービスを受けることができるようになる。
- [0045] システム100は、ICカード発行者121のサービスと、カード記憶領域使用者124のサービスとを単体のICカード116を用いて提供するに当たって、ICカード発行者121及びカード記憶領域使用者124のサービスに係わるファイル・データが記憶される記憶領域に、権限を有しない他人によって不正にデータの書き込み及び書き換えなどが行なわれることを困難にする構成を有している。
- [0046] なお、図2では、それぞれ単数のICカード発行者121、カード記憶領域使用者124及びカード所有者126がある場合を例示したが、これらは、それぞれ複数であってもよい。
- [0047] ICカード116は、その字義通り、カード型のデータ通信装置であつてもよいし、いわゆるICカード機能が実装された半導体チップを内蔵した携帯電話機(あるいはその他の携帯端末やCE機器)として具現化されることもある。また、非接触ICカード機能を搭載したICチップは、RFアナログ・フロントエンドとロジック回路(プロトコル制御、RF変復調、コマンド処理、暗号処理、メモリ管理)を1チップで構成してもよいし、あるいはこれらを分離した2チップ以上のICで構成するようにしてもよい。
- [0048] 図15には、本発明の一実施形態に係るICカード部のハードウェア構成を模式的に示している。同図に示すように、ICカード部は、アンテナ部1001に接続されたアナロ

グ部1002と、デジタル制御部1003と、メモリ1004と、外部インターフェース1005とで構成され、携帯端末1100に内蔵されている。このICカード部は、1チップの半導体集積回路で構成してもよいし、RFアナログ・フロントエンドとロジック回路部を分離して2チップの半導体集積回路で構成してもよい。

- [0049] アンテナ部1001は、図示しないカード読み書き装置との間で非接触データの送受信を行なう。アナログ部1002は、検波、変復調、クロック抽出など、アンテナ部1001から送受信されるアナログ信号の処理を行なう。これらは、ICカード部とカード読み書き装置間の非接触インターフェースを構成する。
- [0050] デジタル制御部1003は、送受信データの処理やその他ICカード内の動作を統括的にコントロールする。デジタル制御部1003は、アドレス可能なメモリ1004をローカルに接続している。メモリ1004は、EEPROM(Electrically Erasable Programmable Read Only Memory)などの不揮発性記憶装置で構成され、電子マネーや電子チケットなどの利用者データを格納したり、デジタル制御部1003が実行するプログラム・コードを書き込んだり、実行中の作業データを保存するために使用することができる。
- [0051] 外部インターフェース1005は、カード読み書き装置(図示しない)と結ぶ非接触インターフェースとは相違するインターフェース・プロトコルにより、デジタル制御部1003が携帯端末1100などの装置と接続するための機能モジュールである。メモリ1004に書き込まれたデータは、外部インターフェース1005を経由して、携帯端末1100に転送することができる。
- [0052] ここで、カード読み書き装置と通信を行なう際に、カード読み書き装置からの受信データをそのまま、あるいは適当な変換規則で変換し、あるいは別のパケット構造に変換して、外部インターフェース1005を介して携帯端末1100に送信する。また逆に、外部インターフェースを介して携帯端末1100から受信したデータをそのまま、あるいは適当な変換規則で変換し、あるいは別のパケット構造に変換して、非接触インターフェースを介してカード読み書き装置に送信する。
- [0053] 本実施形態では、ICカード部は、携帯端末1100に内蔵して用いられることを想定しており、外部インターフェース1005には、UART(Universal Asynchronous

Receiver Transmitter)のような有線インターフェースを使用する。但し、外部インターフェース1005のインターフェース仕様は特に限定されず、有線インターフェースであっても、あるいはBluetooth通信やIEEE. 802. 11などの無線インターフェースであってもよい。

- [0054] ICカード部は、例えば、アンテナ部1001経由で受信されるカード読み書き装置からの受信信号から得られるエネルギーによって駆動することができる。勿論、携帯端末1100側からの供給電力によって、一部又は全部が動作するように構成されていてもよい。
- [0055] 携帯端末1100は、例えば携帯電話機やPDA、パーソナル・コンピュータ(PC)などの情報処理端末に相当する。携帯端末1100は、プログラム制御部1101と、表示部1102と、ユーザ入力部1103とで構成される。
- [0056] プログラム制御部1101は、例えばマイクロプロセッサと、RAMと、ROMで構成され(いずれも図15には図示しない)、マイクロプロセッサは、ROMに格納されたプログラム・コードに従って、RAMを作業領域に用いてさまざまな処理サービスを実行する。処理サービスには、携帯電話機など携帯端末1100本来の機能の他に、ICカード部に対する処理も含まれる。勿論、プログラム制御部1101は、ハード・ディスクなどの外部記憶装置や、その他の周辺装置を備えていてもよい。
- [0057] プログラム制御部1101は、外部インターフェース1005経由で、ICカード部にアクセスすることができる。
- [0058] 表示部1102は、例えば液晶表示ディスプレイで構成され、プログラム制御部1101における処理結果などを画面出力してユーザに通知することができる。
- [0059] ユーザ入力部1103は、キーボードやジョグダイヤル、あるいは表示部1102の表示画面に重畳されたタッチパネルなどで構成され、ユーザが携帯端末1100にコマンドやデータを入力するために使用される。
- [0060] 携帯端末1100内のプログラム制御部1101は、バッテリーなど図示しない主電源からの給電により駆動する。
- [0061] ICカード部が内蔵された携帯端末1100のユーザが携帯端末1100を所定のカード読み書き装置にかざすことにより、ICカード部とカード読み書き装置間の無線通信が

開始され、無線インターフェースとしてのアンテナ部1001及びアナログ部1002を介して、デジタル部1003とカード読み書き装置の間でデータ交換が行なわれる。

[0062] C. ファイル・システム

ICカードが持つ耐タンパ性と認証機能を利用して、価値情報のやり取りなどを含んだセキュリティが要求されるサービスを提供することができる。さらに本実施形態では、単一のメモリ領域上にサービス提供元事業者毎のファイル・システムを割り当て、単一のICカードを複数の事業者で共有し、単一のICカードにより複数のサービスを提供するようにした。

[0063] ICカード内のメモリ領域は、初期状態では、ICカード発行者がメモリ領域全体を管理している。ICカード発行者以外のサービス提供元事業者がメモリ領域から新たなファイル・システムを分割するに際しては、メモリ領域の分割権限と、ICカード発行者に対する認証の双方が要求される。

[0064] メモリ領域が一旦分割されると、ファイル・システムへのアクセスは、元のICカードの発行者ではなく、ファイル・システム自体のサービス提供元事業者への認証が要求される。したがって、ファイル・システム間の境界がファイヤ・ウォールとして機能し、他のファイル・システムからの不正なアクセスを好適に排除することができる。また、ユーザにとっては、各サービス利用時において事業者自らが発行したICカードであるかのような使い勝手を確保することができる。そして、メモリ領域の分割操作を繰り返すことにより、ICカード内のメモリ領域は複数のファイル・システムが共存する構造となる。ファイル・システムの分割は、仮想的なICカードの発行である。

[0065] ここで、図3～図6を参照しながら、ICカード内のメモリ領域の運用形態について説明する。

[0066] 図3には、元のカード発行者が自らのファイル・システムのみを管理しているメモリ領域の状態を示している。元のカード発行者のシステム・コードSC1は、システム・コードの管理機構が付与する。外部機器又はプログラムがカード発行者のファイル・システムにアクセスする場合は、SC1を識別コード(すなわち、要求コマンドの引数)とする。

[0067] 図4には、カード発行者が自らのファイル・システムの空き領域の内で、ある範囲の

メモリを領域管理者に貸与(又は譲渡)することが許可できることを示している。この段階では、まだメモリ領域上のファイル・システムに対して分割が行なわれている訳ではない。カード発行者は、自らのファイル・システムに空き領域はあるうちは、複数の領域管理者に対して、メモリを貸与することを許可できる。例えば、4ビットのシステム・コードでファイル・システムを識別するという実装では、最大16分割(15回まで分割)することができる。

[0068] 図5には、他のサービス提供元事業者が、カード発行者から許可された領域においてメモリ領域を分割し、新たなファイル・システムを生成した状態を示している。この新規ファイル・システムには、システム・コードの管理機構からシステム・コードSC2が付与されている。外部機器又はプログラムが、当該メモリ領域管理者(サービス提供元事業者)の運用するファイル・システムにアクセスする場合は、SC2を識別コード(要求コマンドの引数)とする。

[0069] 図6には、共通領域管理者が、カード発行者から許可された領域において、共通領域のシステム・コードSC0でメモリを分割した状態を示している。外部機器又はプログラムがこの共通領域管理者の運用領域であるファイル・システムにアクセスする場合には、そのシステム・コードSC0を識別コード(要求コマンドの引数)とする。

[0070] ICカードのメモリ領域は、分割操作を繰り返すことにより、図7に示すように複数のファイル・システムが共存する構造となる。元のカード発行者、並びにカード発行者の許可によりICカード上で自己のファイル・システムを取得したサービス提供元事業者は、それぞれ自己のファイル・システムを利用して、エリアやサービスを配設し、自身の事業展開に利用することができる。

[0071] ここで、1つのファイル・システム内での運用形態について説明する。基本的には、どのファイル・システムにおいても同様の動作が実現されるものとする。

[0072] ファイル・システム内には、電子決済を始めとする外部との電子的な価値情報のやり取りなどのアプリケーションを実現するための、1以上のファイルが配置されている。アプリケーションに割り当てられているメモリ領域を「サービス・メモリ領域」と呼ぶ。また、アプリケーションの利用、すなわち該当するサービス・メモリ領域へアクセスする処理動作のことを「サービス」と呼ぶ。サービスには、メモリへの読み出しアクセス、書き

込みアクセス、あるいは電子マネーなどの価値情報に対する価値の加算や減算などが挙げられる。

- [0073] ユーザがアクセス権を持つかどうかに応じてアプリケーションの利用すなわちサービスの起動を制限するために、アプリケーションに対して暗証コードすなわちPINを割り当て、サービス実行時にPINの照合処理を行なうようになっている。また、サービス・メモリ領域へのアクセスは、アプリケーションのセキュリティ・レベルなどに応じて、適宜暗号化通信が行なわれる。
- [0074] 本実施形態では、ICカード内のメモリ領域に設定されているそれぞれのファイル・システムに対して、「ディレクトリ」に類似する階層構造を導入する。そして、メモリ領域に割り当てられた各アプリケーションを、所望の階層の「エリア」に登録することができる。
- [0075] 例えば、一連のトランザクションに使用される複数のアプリケーション、あるいは関連性の深いアプリケーション同士を同じエリア内のサービス・メモリ領域として登録する（さらには、関連性の深いエリア同士を同じ親エリアに登録する）ことによって、メモリ領域のアプリケーションやエリアの配置が整然とし、ユーザにとってはアプリケーションの分類・整理が効率化する。
- [0076] また、ファイル・システムへのアクセス権を階層的に制御するために、アプリケーション毎にPINを設定できる以外に、各エリアに対してもPINを設定することができるようにしている。例えば、あるエリアに該当するPINを入力することにより、照合処理並びに相互認証処理を経て、エリア内のすべてのアプリケーション（並びにサブエリア）へのアクセス権を与えるようにすることもできる。したがって、該当するエリアに対するPINの入力を1回行なうだけで、一連のトランザクションで使用されるすべてのアプリケーションのアクセス権を得ることができるので、アクセス制御が効率化するとともに、機器の使い勝手が向上する。
- [0077] さらに、あるサービス・メモリ領域に対するアクセス権限が単一でないことを許容し、それぞれのアクセス権限毎、すなわちサービス・メモリ領域において実行するサービスの内容毎に、暗証コードを設定することができる。例えば、同じサービス・メモリ領域に対して起動するサービスが「読み出し」と「読み出し及び書き込み」とでは、別々のP

INが設定される。また、電子マネーやその他の価値情報に対する「増額」と「減額」とでは、別々のPINが設定される。また、あるメモリ領域に対する読み出しについてはPINの入力が必要でないが、書き込む場合にはPINの入力を必須とさせることが可能である。

- [0078] 図8には、ファイル・システム内のデータ構造例を模式的に示している。図示の例では、ファイル・システムが持つ記憶空間には、「ディレクトリ」に類似する階層構造が導入されている。すなわち、メモリ領域に割り当てられた各アプリケーションを、所望の階層エリアにサービス・メモリ領域として登録することができる。例えば、一連のトランザクションに使用されるアプリケーションなど、関連性の深いアプリケーション同士を同じエリアに登録する(さらには、関連性の深いエリア同士を同じ親エリアに登録する)ことができる。
- [0079] また、ファイル・システム内に割り当てられたアプリケーション(すなわちサービス・メモリ領域)並びにエリアは暗証コード定義ブロックを備えている。したがって、アプリケーション毎に、あるいはエリア毎にPINを設定することができる。また、ファイル・システムに対するアクセス権は、アプリケーション単位で行なうとともに、並びにエリア単位で行なうことができる。
- [0080] さらに、あるサービス・メモリ領域に対するアクセス権限が単一でなく、実行するサービスの内容毎に、PINを設定することができる。例えば、同じサービス・メモリ領域に対して起動するサービスが「読み出し」と「読み出し及び書き込み」とでは、別々のPINが設定され、また、電子マネーやその他の価値情報に対する「増額」と「減額」とでは、別々のPINが設定される。
- [0081] 照合部は、例えばICカードを利用した非接触データ通信などのプロトコル・インターフェースを介して送られてくるPINを、各アプリケーション又はディレクトリに割り当てられたエリア又はサービス・メモリ領域に設定されている暗証コードと照合して、一致するメモリ領域に対するアクセスを許可する。アクセスが許可されたメモリ領域は、プロトコル・インターフェースを介して読み書きが可能となる。
- [0082] 図9には、ファイル・システムの基本構成を示している。図8を参照しながら既に説明したように、ファイル・システムに対して、「ディレクトリ」に類似する階層構造が導入さ

れ、所望の階層のエリアに、アプリケーションに割り当てられたサービス・メモリ領域を登録することができる。図9に示す例では、エリア0000定義ブロックで定義されるエリア0000内に、1つのサービス・メモリ領域が登録されている。

- [0083] 図示のサービス・メモリ領域は、1以上のユーザ・ブロックで構成される。ユーザ・ブロックはアクセス動作が保証されているデータ最小単位のことである。このサービス・メモリ領域に対しては、サービス0108定義ブロックで定義されている1つのサービスすなわちサービス0108が適用可能である。
- [0084] エリア単位、並びにアプリケーション単位でアクセス制限を行なう以外に、サービスの種類毎に暗証コードを設定して、サービス単位でアクセス制限を行なうことができる。アクセス制限の対象となるサービスに関する暗証コード設定情報は、暗証コード専用のサービス(すなわち「暗証コード・サービス」)として定義される。図9に示す例では、サービス0108に関する暗証コードが暗証コード・サービス0128定義ブロックとして定義されている。その暗証コード・サービスの内容は暗証コード・サービス・データ・ブロックに格納されている。
- [0085] サービス0108に対する暗証コード・サービスが有効になっている場合、サービス0108を起動してそのユーザ・ブロックに読み出し又は書き込み動作を行なう前に、暗証コード・サービス0128を使用した暗証コードの照合が必要となる。具体的には、暗号化あり読み書き(Read/Write)コマンドを使用する場合は、相互認証前にサービス0108に対する暗証コードすなわちPINの照合を行なう。
- [0086] また、アプリケーションに割り当てられたサービス・メモリ領域を所望の階層のエリアに登録するとともに、エリアを階層化する(関連性の深いエリア同士を同じ親エリアに登録する)ことができる。この場合、エリア毎にPINを設定することにより、エリアをアクセス制限の単位とすることができる。図10には、ICカードのメモリ空間においてエリアが階層化されている様子を示している。同図に示す例では、エリア0000定義ブロックで定義されているエリア0000内に、エリア1000定義ブロックで定義されている別のエリア1000が登録されている。
- [0087] 図10に示す例では、さらにエリア1000内には、2つのサービス・メモリ領域が登録されている。一方のサービス・メモリ領域に対しては、サービス1108定義ブロックで定

義されているサービス1108と、サービス110B定義ブロックで定義されているサービス110Bが適用可能である。このように、1つのサービス・メモリ領域に対してサービス内容の異なる複数のサービスを定義することを、本明細書中では「オーバーラップ・サービス」と呼ぶ。オーバーラップ・サービスにおいては、同じサービス・エリアに対して、入力したPINに応じて異なるサービスが適用されることになる。また、他方のサービス・メモリ領域に対しては、サービス110C定義ブロックで定義されているサービス110Cが適用可能である。

- [0088] 各サービス・メモリ領域に設定されているサービスを起動してそのユーザ・ブロックに読み出し又は書き込み動作を行なうことができる。勿論、図9を参照しながら説明したように、サービス毎に暗証コード・サービスを定義することができる。この場合、サービスに対する暗証コード・サービスが有効になっているときには、暗証コード・サービスを使用したPINの照合を行なってからサービスの起動が許可される。
- [0089] また、複数のサービスに対して共通のPINを設定したい場合には、これらサービスを含むエリアを作成し、このエリアに対して共通の暗証コード・サービスを適用することができる。
- [0090] 図10に示す例では、エリア1000に関する暗証コードが、暗証コード・サービス1020定義ブロックとして定義されている。その暗証コード・サービスの内容は暗証コード・サービス・データ・ブロックに格納されている。
- [0091] エリア1000に対する暗証コード・サービスが有効(後述)になっている場合、暗証コード・サービス1020を使用した暗証コードの照合を行なった後に、エリア1000内の各サービスを起動してそのユーザ・ブロックに読み出し又は書き込み動作を行なうことが可能となる。
- [0092] 図11には、内部メモリに複数のファイル・システムを設けることができるICカード内のファームウェアの機能構成を模式的に示している。
- [0093] インターフェース制御部は、非接触ICカード・インターフェースによるカード・リーダ／ライタとの通信、カード・リーダ／ライタとしての通信、有線インターフェースを介した通信、その他のI/Oインターフェースを介した通信などのプロトコル制御を行なう。
- [0094] コマンド制御部は、インターフェース制御部を介して外部から受け取ったコマンドの

処理や、外部に対するコマンド発行、コマンドの検査などを行なう。

[0095] セキュリティ制御部は、メモリ領域若しくはメモリ領域内の各ファイル・システムへアクセスする際の認証処理や、ファイル・システム内のディレクトリやサービスを利用する際のPIN照合などのセキュリティ処理を実現する。

[0096] ファイル・システム制御部は、上述したようなメモリ領域からファイル・システムへの分割(並びに分割の解消)などファイル・システム管理や、ファイル・システム内のディレクトリ構造の管理などを行なう。

[0097] モード管理部は、全ファイル・システム並びに個別のファイル・システムのモードの管理を行なう。ここで言うモードには、ファイル・システムの利用停止や利用再開などの状態が含まれる。

[0098] この他、起動制御やROM管理、パラメータ管理、不揮発性メモリ管理、パッチ制御など、ICカード内の各ハードウェア制御用のファームウェアも含まれている。

[0099] D. ファイルのアーカイブ

ICカードに担持されているデータのバックアップをとることが必要となってくる。図12には、ICカード内のファイルやディレクトリをアーカイブするための仕組みを図解している。

[0100] 上述したようにICカード内のメモリ空間には、ディレクトリに類似する階層構造が導入されている。アーカイブ・ファイル作成部は、バックアップを取ることが指定されたファイル又はディレクトリをアーカイブするためのアーカイブ・ファイルを作成する。アーカイブ・ファイルの形式は特に限定されない。そして、アーカイブ・ファイルの展開先となる端末を識別する端末IDを指定して、アーカイブ・ファイルを保管装置に格納する。これによって、ICカード内のデータのバックアップが実現する。

[0101] 保管装置は、耐タンパ性があり、格納しているアーカイブ・ファイルが外部に不正に漏洩することはない。そして、保管装置は、アーカイブ・ファイルを端末IDで指定されている端末へ転送する。

[0102] 指定された端末では、アーカイブ・ファイルを展開して元のファイルやディレクトリを復元し、利用が再開される。これによって、ICカード内のデータを正しい相手に移動することができる。

- [0103] 一方、ICカード内のファイルやディレクトリへのアクセスをカウンタで管理する仕組みを導入し、アーカイブ・ファイルを保管場所にアーカイブした後は元のファイルのカウンタ値を消滅させてアクセスできないようにすることで、移動後のデータの2重化を防止している。
- [0104] 本実施形態では、各ファイルへのアクセス回数を管理する特殊ファイルであるカウンタ・ファイルをメモリ内若しくはディレクトリ内に配置するようにした。カウンタ・ファイルには、メモリ内若しくはディレクトリ内の各ファイルについてのアクセス回数の上限值が記載されている。
- [0105] また、ファイル連携指定子を導入して、2以上のファイルの連携関係を設定できるようにした。ファイル連携指定子で指定されている2以上のファイルには、双方同時にオープンしなければならない、すなわち同時に認証を経なければいずれのファイルもオープンできないという制限が課される。アーカイブ・ファイルが作成されたファイルは、ファイル連携指定ファイルにより、カウンタ・ファイルと連携指定される。
- [0106] 図13には、ファイルの連携指定したファイル・システム内の基本構成を模式的に示している。図示の例では、2以上のファイルの同時認証を指定するファイル連携指定子は、ファイル・システム内の他のファイルと同様、ファイル形式で構成されている。但し、別の形態でファイル連携指定子を定義するようにしても構わない。
- [0107] 図示の例では、ファイル・システム内には、ファイル1～3と、カウンタ・ファイルが配置されている。ファイル1～3には、ICカード発行者が全カードに共通する対称鍵がそれぞれ設定されている。また、カウンタ・ファイルには個別鍵が設定されている。
- [0108] また、図示の例では、ファイル連携指定ファイルが配置されているが、これは同時に認証できるファイルの組み合わせを指定する特殊ファイルである。ファイル連携指定ファイル自体は、他のファイルと同様に、ICカード発行者がすべてのICカードに共通の対称鍵で認証を行なうように設定されている。
- [0109] ファイル連携指定ファイルは、アーカイブを行なうファイル2とカウンタ・ファイルとの連携、すなわちファイル2はカウンタ・ファイルと同時にオープンしなければならないことを規定している。
- [0110] 以下では、ファイルをオープンするときに必要な認証鍵は、ファイルに対して指定さ

れている鍵の組合せを所定の関数 f で演算することによって得られるものとする。

- [0111] ファイル1は、いずれのファイル連携指定子によっても規定されていない。したがって、ファイル1自体に設定された対称鍵 K_{s1} だけで相互認証を行なえば、ファイルを開くことができる。この場合の認証鍵は以下の通りとなる。

[0112]
$$\text{認証鍵 } K_{\text{AUTH1}} = f(\text{ファイル1の対称鍵 } K_{s1})$$

- [0113] また、ファイル2は、ファイル2に設定された対称鍵で相互認証することはできず、ファイル連携指定ファイルの設定に従い、カウンタ・ファイルと同時に相互認証しなければならない。このときに利用する相互認証鍵は、ファイル2の対称鍵 K_{s2} とカウンタ・ファイルの個別鍵 K_p を組み合わせた結果を利用するので、個別鍵となる。

[0114]
$$\text{認証鍵 } K_{\text{AUTH2}} = f(\text{ファイル2の対称鍵 } K_{s2}, \text{カウンタ・ファイルの個別鍵 } K_p)$$

- [0115] 認証鍵 K_{AUTH2} を以ってファイル2にアクセスした場合、カウンタ・ファイルが同時にオープンされ、カウンタ値がデクリメントされる。カウンタ値が0xffffであれば、カウンタ・ファイルはいつでも開くことができる。これに対し、カウンタ値が0であれば、カウンタ・ファイルを開くことができないため、連携指定されているファイル2もオープンすることはできない。

- [0116] 図16には、ファイル・システム内でファイルの連携関係を設定するための処理手順をフローチャートの形式で示している。ここでは、アーカイブの対象となるファイルと、そのファイルへのアクセス回数を制限するカウンタ・ファイルの連携関係を形成することを想定している。

- [0117] まず、アーカイブの対象となるファイルへのアクセス回数を記述したカウンタ・ファイルを作成し(ステップS1)、続いてこのカウンタ・ファイルをオープンするための個別鍵を設定する(ステップS2)。

- [0118] そして、アーカイブの対象となるファイルとカウンタ・ファイルとの連携関係を記述したファイル連携指定ファイルを作成し(ステップS3)、このファイル連携指定ファイルにアクセスするための鍵を設定する(ステップS4)。この鍵には、全ICカード共通で使用する対称鍵を利用する(前述)。

- [0119] また、図17には、ファイル・システム内でファイル連携関係が指定されたファイルに対してアクセスするための処理手順をフローチャートの形式で示している。ここでは、

アーカイブの対象となるファイルと、そのファイルへのアクセス回数を制限するカウンタ・ファイルの連携関係を形成することを想定している。

- [0120] ファイル・システムにアクセスすると、まず、当該ファイル・システム内でファイル連携指定ファイルの有無をチェックする(ステップS11)。ここで、ファイル連携指定ファイルが存在しない場合には、ファイル・システム内の各ファイルに対して単独の認証処理でアクセスすることが可能であり、ファイル毎に設定されている鍵を用いた認証処理を経て行なわれる(ステップS19)。本実施形態では、ファイル連携指定ファイルの鍵はすべてのICカードで共通の対称鍵としている。
- [0121] 一方、ファイル連携指定ファイルが存在する場合には、さらにファイル連携指定ファイル内の記述を確認して(ステップS12)、アクセスしようとしているファイルに対しファイル連携関係が設定されているかどうかをチェックする(ステップS13)。
- [0122] ここで、アクセスしようとしているファイルに関してファイル連携関係が設定されていなければ、当該ファイルに対して単独の認証処理でアクセスすることが可能である。すなわち、当該ファイルに設定されている個別鍵を用いた認証処理を経てアクセスすることができる(ステップS20)。本実施形態では、同じファイルについてはすべてのICカードで共通の対称鍵を使用している。
- [0123] また、アクセスしようとしているファイルに関してファイル連携関係が設定されている場合には(ステップS13)、アクセスしようとしているファイルと、これと連携関係にあるファイルそれぞれの鍵を用いて認証鍵を生成して、同時認証処理を行なう(ステップS14)。本実施形態では、連携関係にあるファイルは、アクセス対象となるファイルへのアクセス回数を記述したカウンタ・ファイルであり、個別鍵が設定されている。したがって、アクセス対象となるファイル自体には全ICカードに共通の対称鍵を使用しているとしても、カウンタ・ファイルの個別鍵を知らなければ同時認証できないので、アーカイブ・ファイルを勝手に操作できない。
- [0124] そして、同時認証に成功すると、続いてカウンタ・ファイルをオープンして、カウンタ値を確認する(ステップS15)。カウンタ値がまだ残っていれば(ステップS16)、アクセス対象となるファイルへのアクセスが可能であり、ファイルのオープンを許可するとともに(ステップS17)、カウンタ値を1だけデクリメントする(ステップS18)。これに対し、カ

ウンタ値が既に消滅している場合には、ファイルのオープンが許可されない(ステップS21)。

- [0125] 上述したようなファイル連携関係を指定するという仕組みを利用することによって、すべてのICカードに共通の対称鍵が割り当てられるファイルであっても、記憶先のファイル・システム内において個別鍵が与えられたファイルとの連携関係を設定することで、同時認証しなければならない。したがって、他のICカードを所持して知り得た共通鍵を用いて、別のICカードの同じファイルにアクセスするという不正行為を制限することができる。
- [0126] また、ファイル・システム内にファイルを記憶する際に、カウンタ・ファイルとファイル連携を指定することによって、当該ファイル・システム内におけるファイルへの回数を自在に設定することができる。例えば、アーカイブしようとするファイルに関し、アーカイブする直前にカウンタ値を1にしたカウンタ・ファイルとファイル連携の指定を行なっておく。この場合、アーカイブした時点でカウンタ値が消滅するので、アーカイブ後は、カウンタ・ファイルに認証してカウンタ値を書き換えない限りは、ファイルにアクセスすることはできない。これにより、セキュアなファイルの移動が実現する。
- [0127] ICカード内のメモリ領域に展開されるファイル・システムにディレクトリ構造を導入できる点は既に述べた通りである。この場合、ディレクトリに対しても、ファイル連携指定の仕組みを適用することができる。図14には、ディレクトリ内のファイル、あるいはディレクトリとカウンタ・ファイルを連携させているファイル・システム内の構成を模式的に示している。
- [0128] ディレクトリ1以下では、ファイル1-1、ファイル1-2、ファイル1-3、カウンタ・ファイル1、並びにファイル連携指定ファイル1が配置されている。
- [0129] ファイル1-1、ファイル1-2、ファイル1-3には、ICカード発行者が全カードに共通する対称鍵がそれぞれ設定されている。また、カウンタ・ファイル1には個別鍵が設定されている。また、ファイル連携指定ファイル1は、ICカード発行者がすべてのICカードに共通の対称鍵で認証を行なうように設定されている。
- [0130] ファイル連携指定ファイル1は、同時に認証できるファイルの組み合わせを指定する特殊ファイルであるが、ここでは、ファイル1-1とカウンタ・ファイル1との連携、すな

わちファイル1-1はカウンタ・ファイル1と同時にオープンしなければならないことを規定している。

- [0131] したがって、ファイル1-2及びファイル1-3はそれぞれの対称鍵のみを用いた単独認証が可能であるのに対し、ファイル1-1は、単独認証することはできず、カウンタ・ファイル1と同時に相互認証しなければならない。このときに利用する相互認証鍵は、ファイル1-1の対称鍵 K_{s1-1} と個別鍵ファイル1の個別鍵 K_{p1} を組み合わせた結果を利用するので、個別鍵となる。
- [0132] 認証鍵 $K_{AUTH} = f(\text{ファイル1-1の対称鍵 } K_{s1-1}, \text{カウンタ・ファイル1の個別鍵 } K_{p1})$
- [0133] ファイル1-1をオープンした場合、カウンタ・ファイル1が同時にオープンされ、カウンタ値がデクリメントされる。カウンタ値が0xffffであれば、カウンタ・ファイルはいつでも開くことができる。これに対し、カウンタ値が0であれば、カウンタ・ファイルを開くことができないため、連携指定されているファイル1-1もオープンすることはできない。
- [0134] 一方、ディレクトリ2以下では、ファイル2-1、ファイル2-2、ファイル2-3、カウンタ・ファイル2、並びにファイル連携指定ファイル2が配置されている。
- [0135] ファイル2-1、ファイル2-2、ファイル2-3には、ICカード発行者が全カードに共通する対称鍵がそれぞれ設定されている。また、カウンタ・ファイル2には個別鍵が設定されている。また、ファイル連携指定ファイル2は、一般ファイルと同様に、ICカード発行者がすべてのICカードに共通の対称鍵で認証を行なうように設定されている。
- [0136] ファイル連携指定ファイル2は、同時に認証できるファイルの組み合わせを指定する特殊ファイルであるが、ここでは、ディレクトリ2とカウンタ・ファイル2との連携、すなわちディレクトリ2はカウンタ・ファイル2と同時にオープンしなければならないことを規定している。
- [0137] したがって、ディレクトリ2以下のすべての一般ファイルは単独認証することができず、ディレクトリ2はカウンタ・ファイル2と同時に相互認証しなければならない。
- [0138] ディレクトリ2をオープンした場合、カウンタ・ファイル2が同時にオープンされ、カウンタ値がデクリメントされる。カウンタ値が0xffffであれば、カウンタ・ファイルはいつでも開くことができる。これに対し、カウンタ値が0であれば、カウンタ・ファイルを開くことができないため、連携指定されているディレクトリ2もオープンすることはできない。

- [0139] ディレクトリに関してカウンタ・ファイルと連携させる場合、そのファイル連携関係を設定する処理手順は、図16に示したフローチャート中のステップS3において、ファイル連携指定ファイルでディレクトリとカウンタ・ファイルの連携関係を記述する、と読み換えればよい。また、ファイル連携関係が指定されたディレクトリに対してアクセスするための処理手順は、図17に示したフローチャート中のステップS11において、アクセス先となるディレクトリ内でファイル連携指定ファイルの有無をチェックすると読み換え、以降の認証及びアクセスの対象を特定のファイルではなくディレクトリ全体として読み換えればよい。
- [0140] このようにして、1以上のディレクトリ、又は1以上のファイルをアーカイブする機能を実現することができる。アーカイブするときには、以下の2つのオプションがある。これにより、ファイルのバックアップ又はコピーを実現することができる。
- [0141] (1)アーカイブしたデータは、アーカイブ時に指定されたIDを持つ端末(ファイル・システム)でしか展開することができない。
- (2)アーカイブしたデータは、任意のファイル・システムにて展開することができる。
- [0142] 例えば、ディレクトリにカウンタ・ファイルを連携させる。ディレクトリをオープンすると、カウンタ・ファイルのカウンタがデクリメントされる。ディレクトリをアーカイブする前のカウンタ値が1の場合、アーカイブ後にはカウンタが0になる。このため、認証手続を経てカウンタ・ファイルにアクセスしてカウンタ値を書き換えない限りは、ディレクトリにアクセスすることはできない。これにより、ディレクトリやファイルの移動が実現する。
- [0143] ディレクトリがルート・ディレクトリの場合、ファイル・システム全体をバックアップ又はコピー又は移動することができる。

産業上の利用可能性

- [0144] 以上、特定の実施形態を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施形態の修正や代用を成し得ることは自明である。
- [0145] 本明細書では、ICカード若しくはICチップに内蔵されるメモリ上に展開されたファイル空間を例にとり、ファイルを安全にアーカイブしバックアップをとる実施形態について説明してきたが、本発明の要旨はこれに限定されるものではない。例えば、ICカー

ドやICチップ以外のメモリ装置上で同種のファイル・システムのアーカイブやアーカイブしたファイル・システムのアクセス管理を行なう場合に、本発明を適用し同様の作用効果を得ることができる。

- [0146] 要するに、例示という形態で本発明を開示してきたのであり、本明細書の記載内容を限定的に解釈するべきではない。本発明の要旨を判断するためには、請求の範囲の記載を参酌すべきである。

請求の範囲

- [1] 無線又は有線伝送路を介してデータを送受信する通信部と、
前記通信部で送受信するデータを処理するデータ処理部と、
前記データ処理部により処理されたファイルを配置するメモリ空間と、
バックアップする1以上のファイルについてのアーカイブ・ファイルを、該アーカイブ・ファイルの展開先の識別情報を付して作成するアーカイブ・ファイル作成手段と、
を具備することを特徴とする情報管理装置。
- [2] アーカイブ・ファイルを作成したファイルへのアクセスを管理するアクセス管理手段をさらに備える、
ことを特徴とする請求項1に記載の情報管理装置。
- [3] 同時にオープンすべきファイルを連携指定するファイル連携指定手段をさらに備え、
アーカイブ・ファイルを作成したファイルと、該ファイルへのアクセス管理情報を記述したアクセス管理情報ファイルとを前記ファイル連携指定手段により連携指定し、
前記アクセス管理手段は、アーカイブ・ファイルを作成したファイルへのアクセスが行なわれた際に、アクセス管理情報ファイルを同時にオープンし、アクセス管理情報に基づいてアクセス管理を行なうとともに、アクセス管理情報の内容を更新する、
ことを特徴とする請求項2に記載の情報管理装置。
- [4] 前記アクセス管理情報ファイルは、アクセス管理情報としてアーカイブ・ファイルを作成したファイルへのカウンタ値を記述し、
前記アクセス管理手段は、アクセス管理情報ファイルをオープンする度にカウンタ値をデクリメントする、
ことを特徴とする請求項3に記載の情報管理装置。
- [5] 前記メモリ空間ではディレクトリ構造が採用され、
前記アーカイブ・ファイル作成手段は、バックアップするディレクトリについてのアーカイブ・ファイルを、該アーカイブ・ファイルの展開先の識別情報を付して作成する、
ことを特徴とする請求項1に記載の情報管理装置。
- [6] メモリ空間に配置されたファイルを管理する情報管理方法であって、

無線又は有線伝送路を介してデータを送受信する通信ステップと、
前記通信ステップにより送受信するデータを処理するデータ処理ステップと、
前記データ処理ステップにより処理されたファイルを前記メモリ空間に配置するステップと、

バックアップする1以上のファイルについてのアーカイブ・ファイルを、該アーカイブ・ファイルの展開先の識別情報を付して作成するアーカイブ・ファイル作成ステップと、

を具備することを特徴とする情報管理方法。

- [7] アーカイブ・ファイルを作成したファイルへのアクセスを管理するアクセス管理ステップをさらに備える、
ことを特徴とする請求項6に記載の情報管理方法。

- [8] 同時にオープンすべきファイルを連携指定するファイル連携指定ステップをさらに備え、

アーカイブ・ファイルを作成したファイルと、該ファイルへのアクセス管理情報を記述したアクセス管理情報ファイルとを前記ファイル連携指定ステップにより連携指定し、

前記アクセス管理ステップでは、アーカイブ・ファイルを作成したファイルへのアクセスが行なわれた際に、アクセス管理情報ファイルを同時にオープンし、アクセス管理情報に基づいてアクセス管理を行なうとともに、アクセス管理情報の内容を更新する、

ことを特徴とする請求項7に記載の情報管理方法。

- [9] 前記アクセス管理情報ファイルは、アクセス管理情報としてアーカイブ・ファイルを作成したファイルへのカウンタ値を記述し、

前記アクセス管理ステップでは、アクセス管理情報ファイルをオープンする度にカウンタ値をデクリメントする、

ことを特徴とする請求項8に記載の情報管理方法。

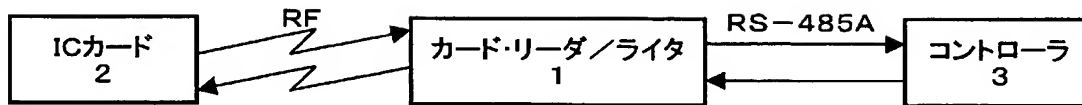
- [10] 前記メモリ空間ではディレクトリ構造が採用され、

前記アーカイブ・ファイル作成ステップでは、バックアップするディレクトリについてのアーカイブ・ファイルを、該アーカイブ・ファイルの展開先の識別情報を付して作成

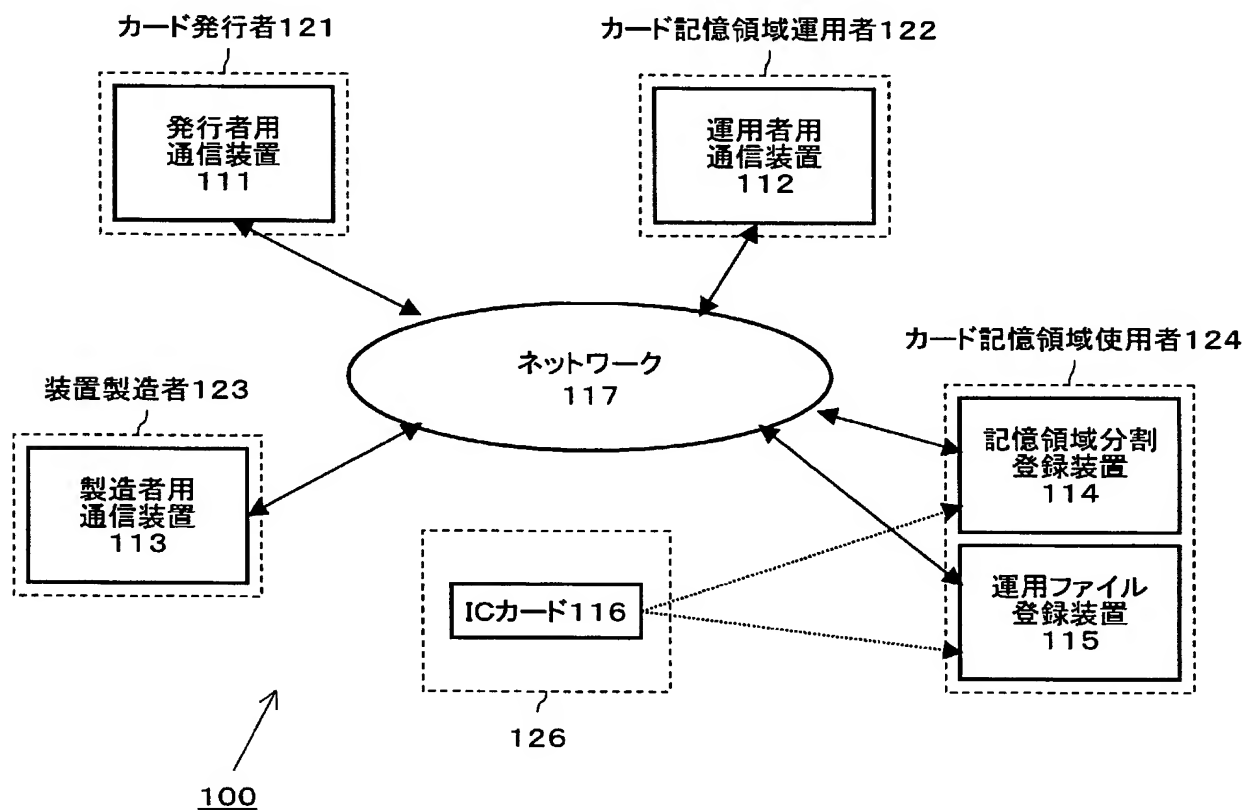
する、

ことを特徴とする請求項6に記載の情報管理方法。

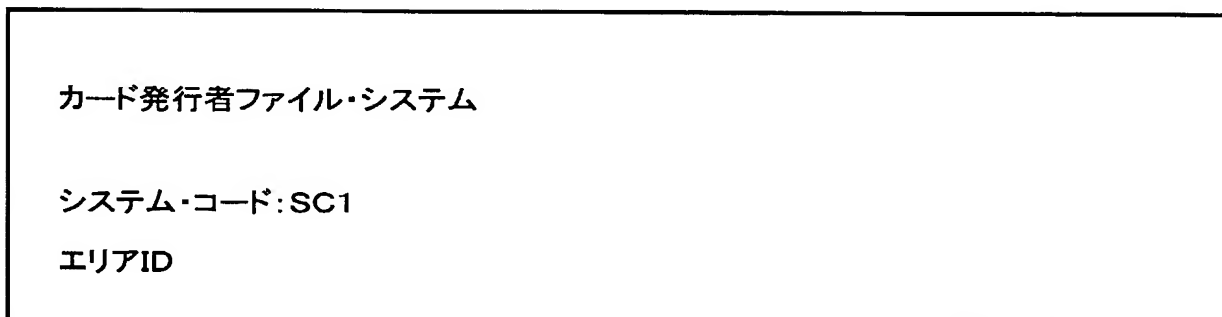
[図1]



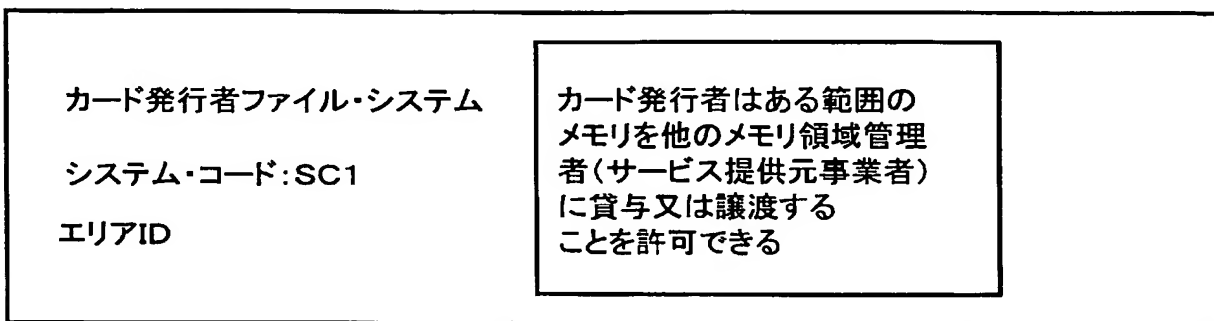
[図2]



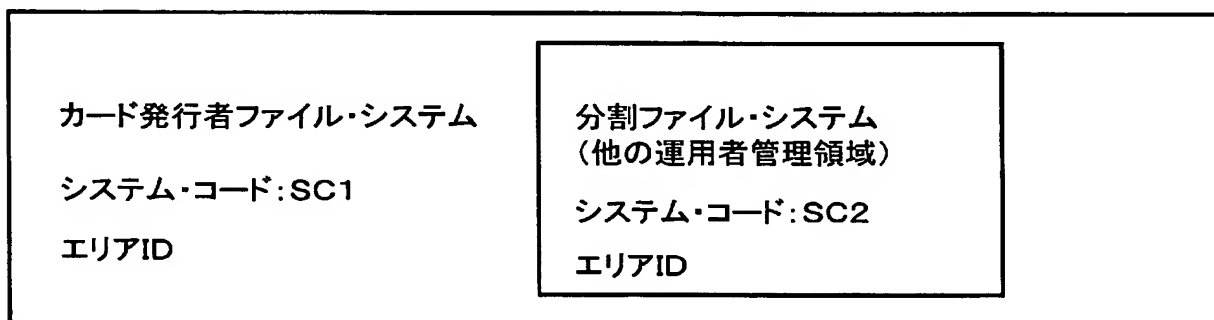
[図3]



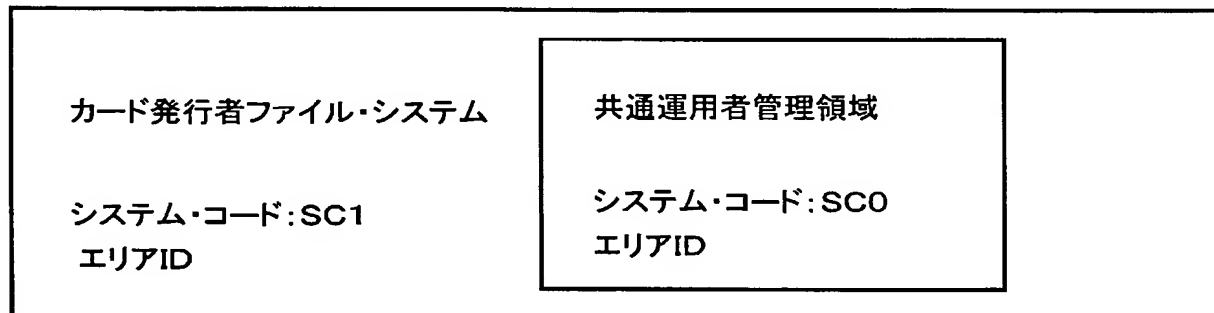
[図4]



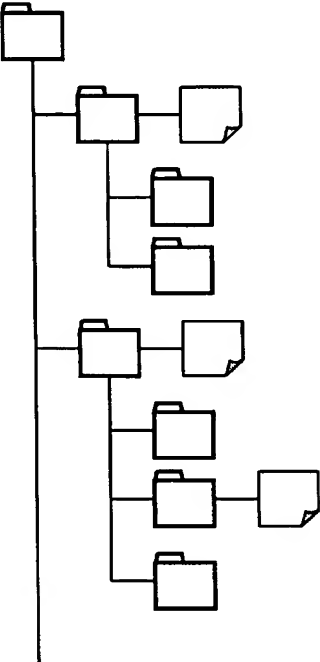
[図5]



[図6]

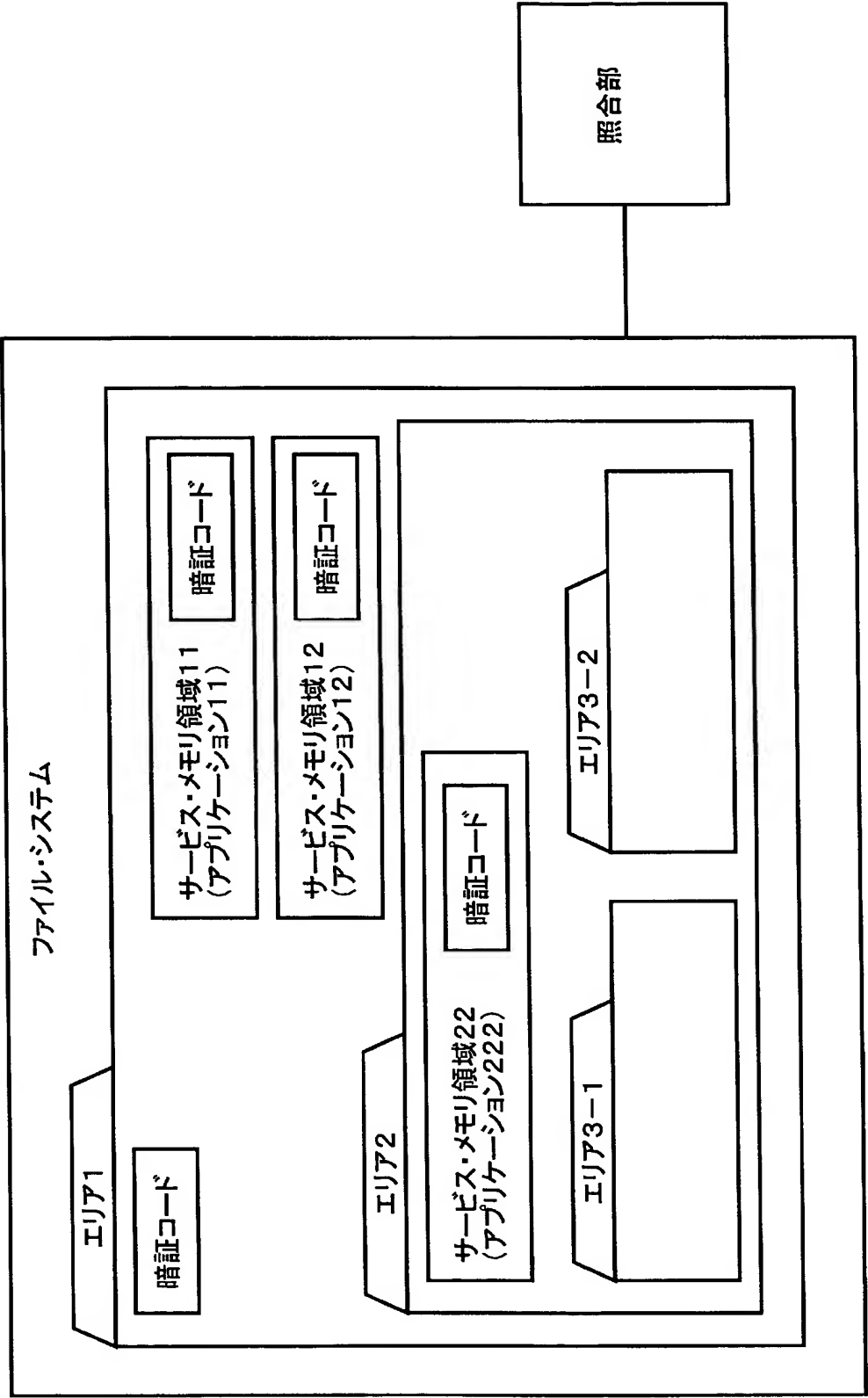


[図7]

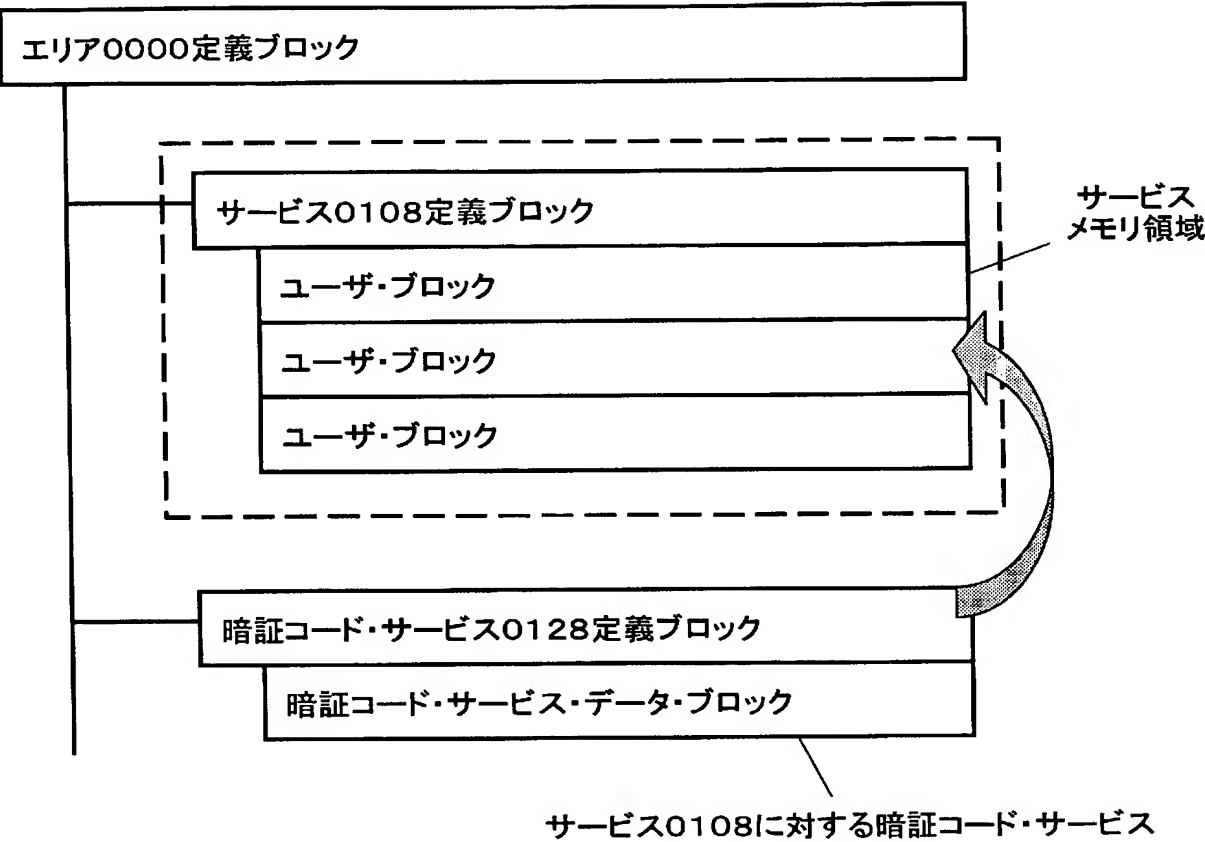
ファイル・システム#0	#1	#1	#1
システム・コードSD#0	SD#1	SD#1	SD#1
エリアID#0	ID#1	ID#1	ID#1
			

.....

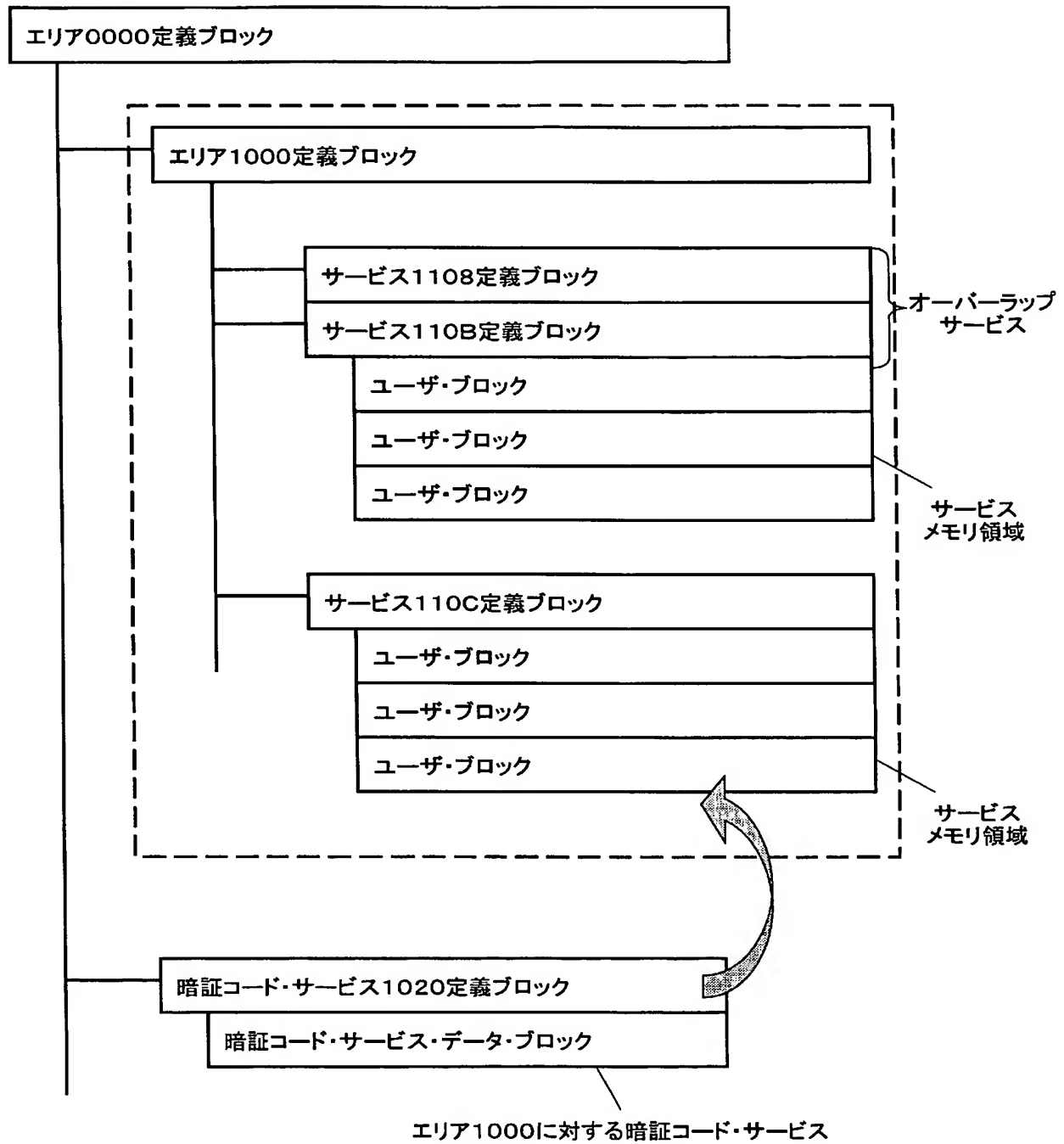
[図8]



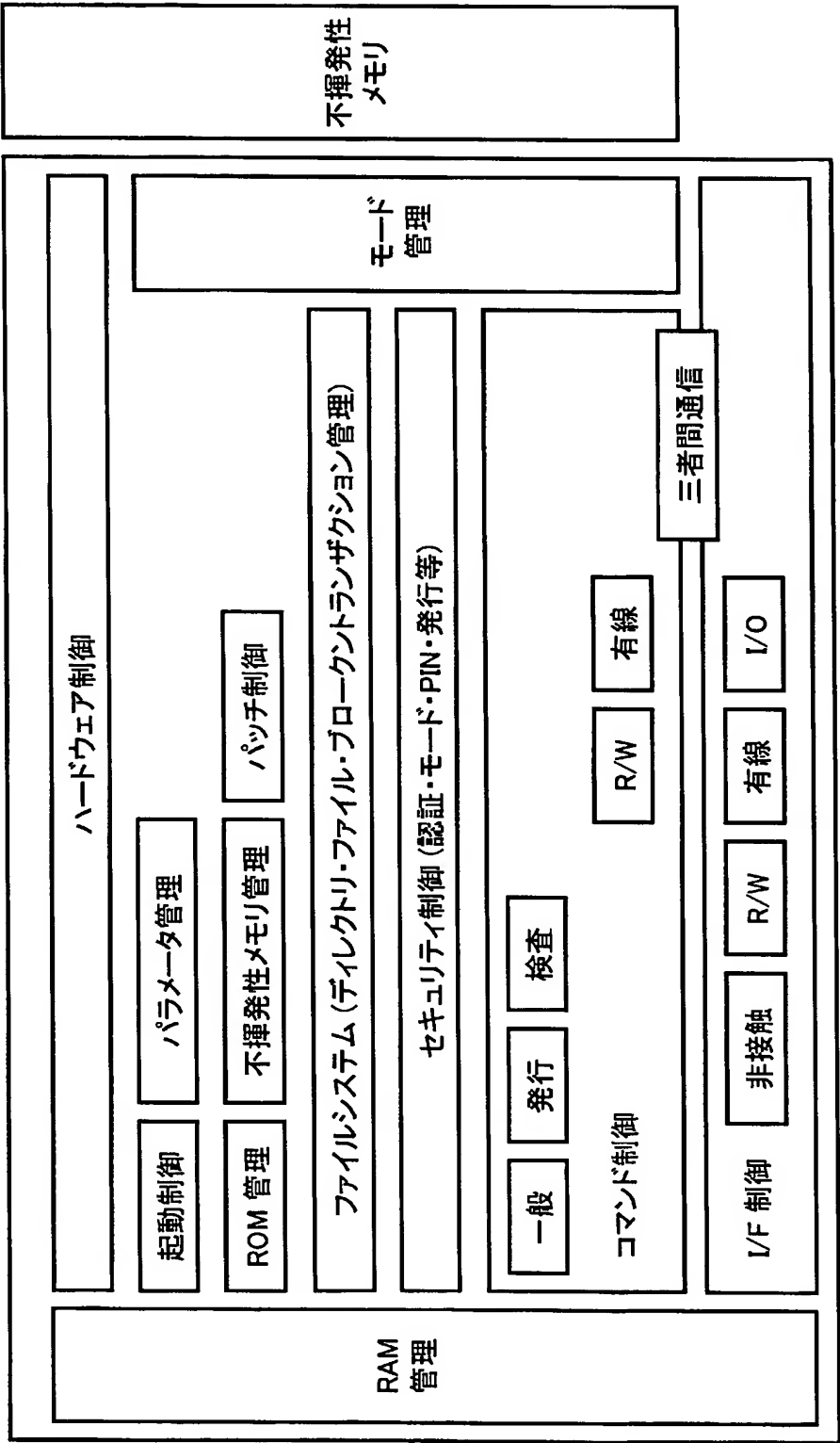
[図9]



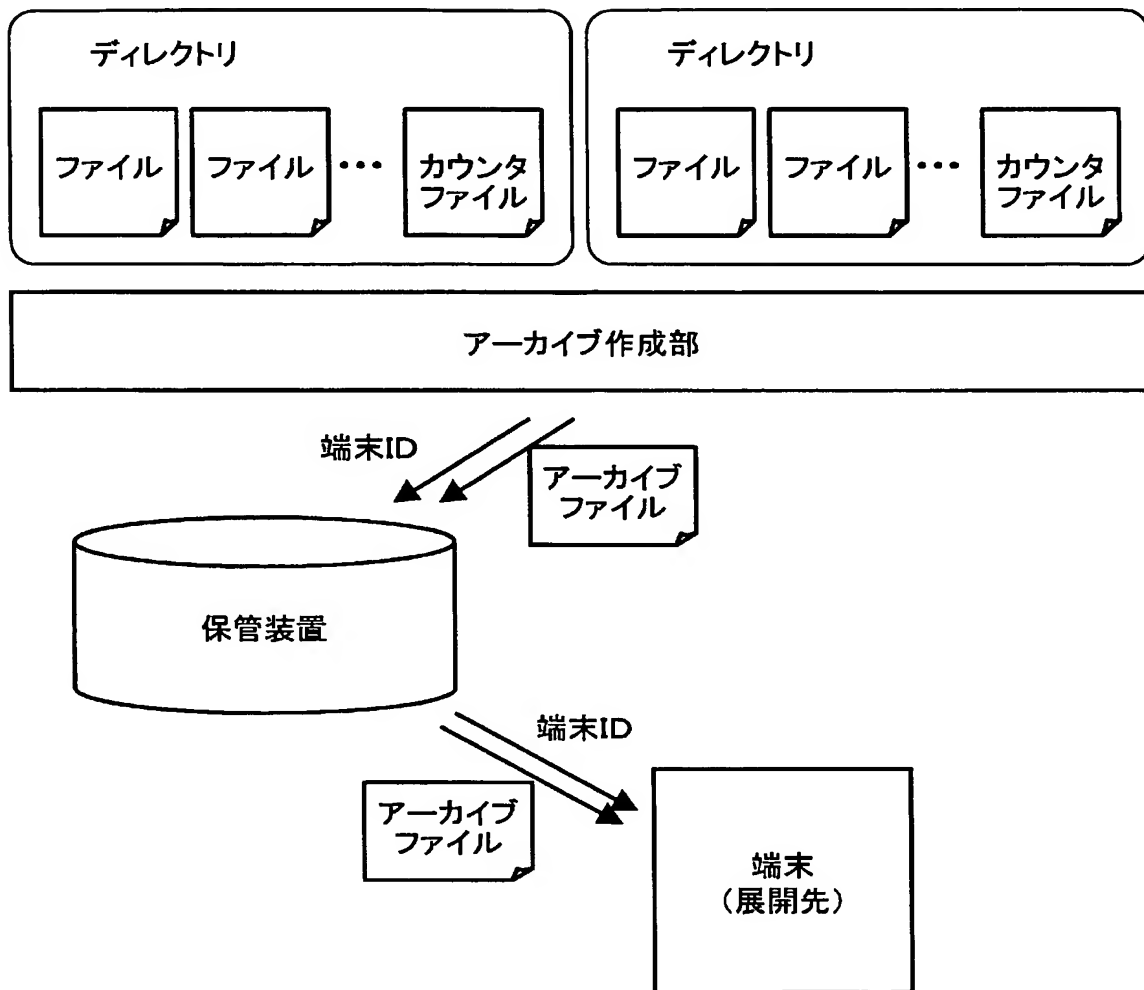
[図10]



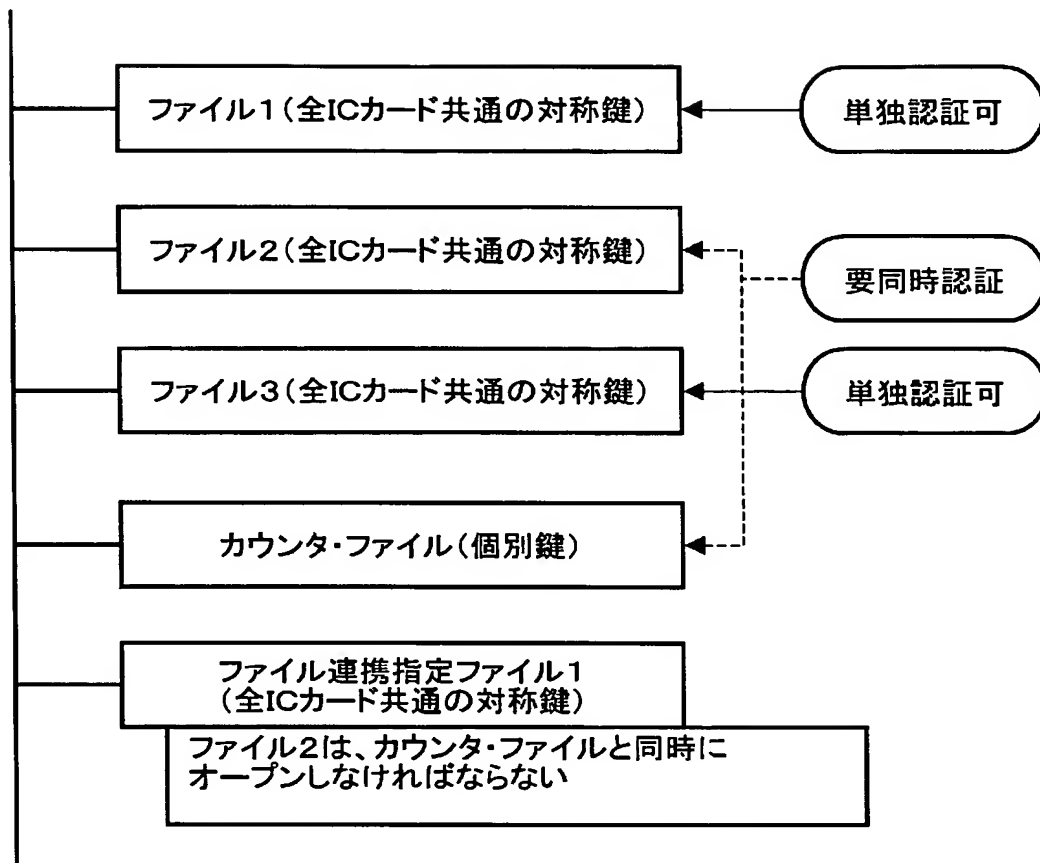
[図11]



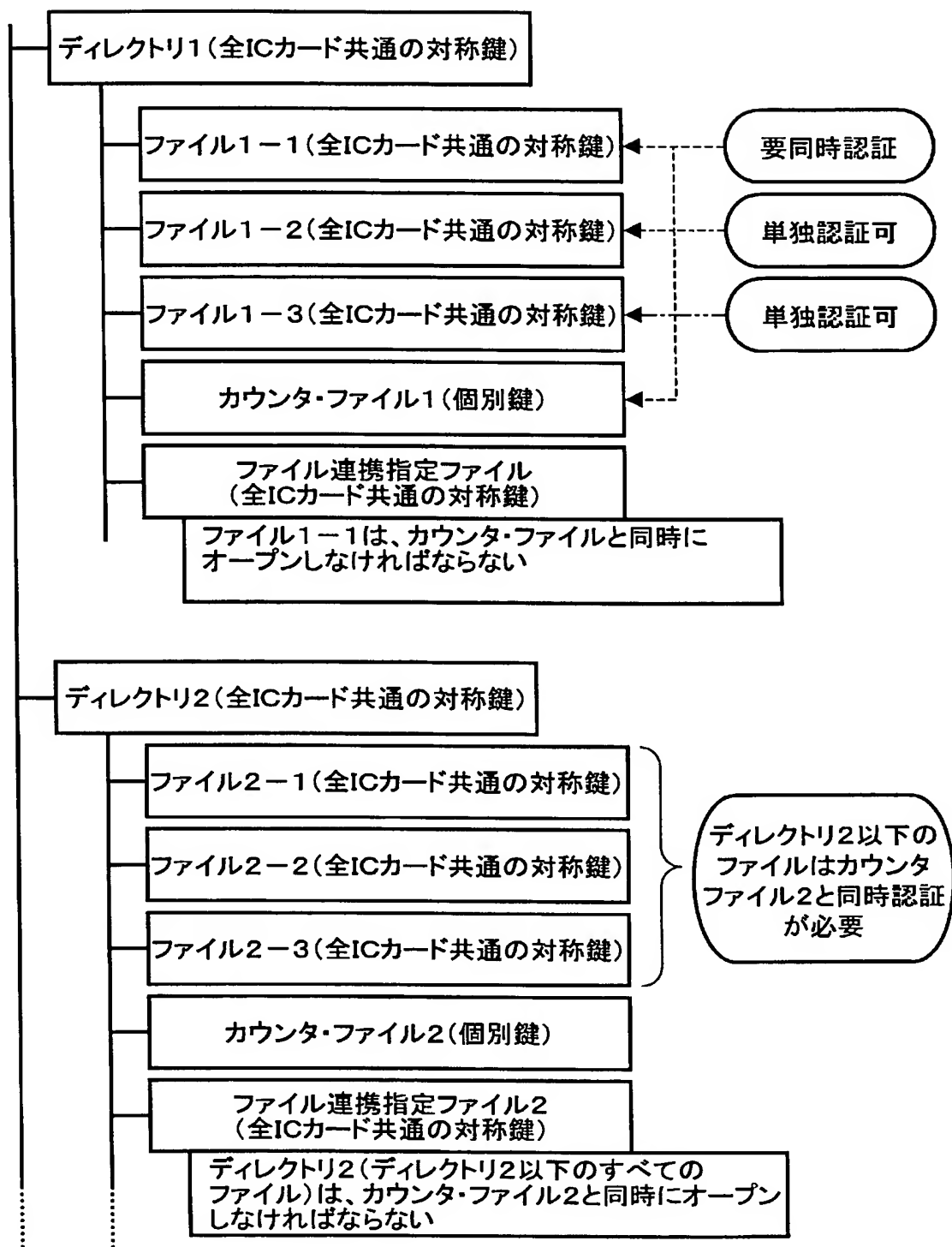
[図12]



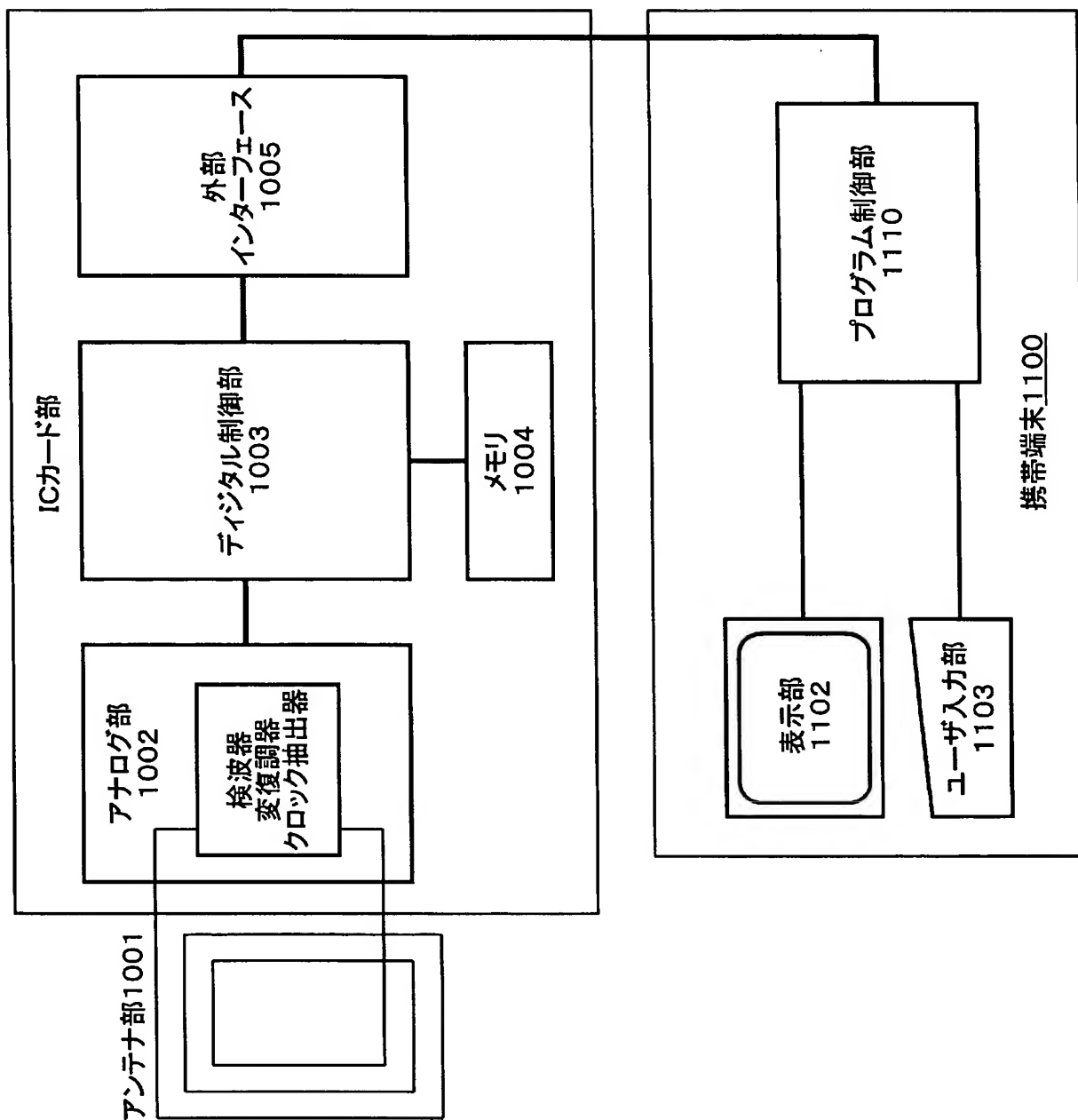
[図13]



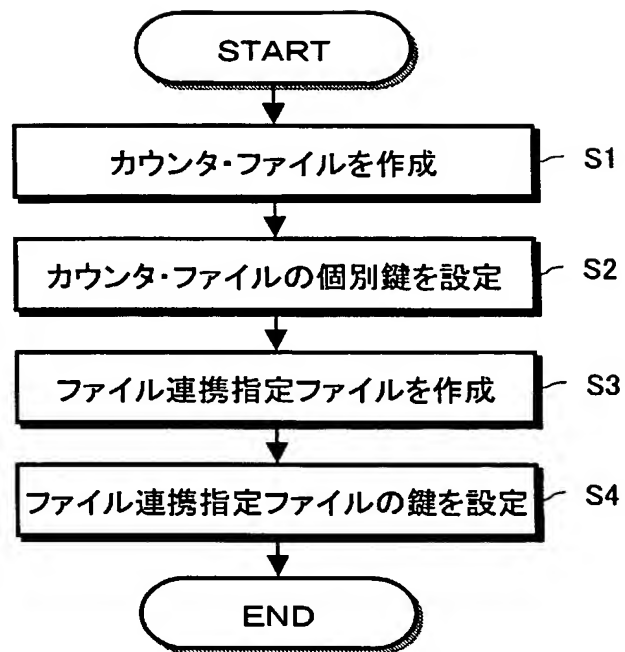
[図14]



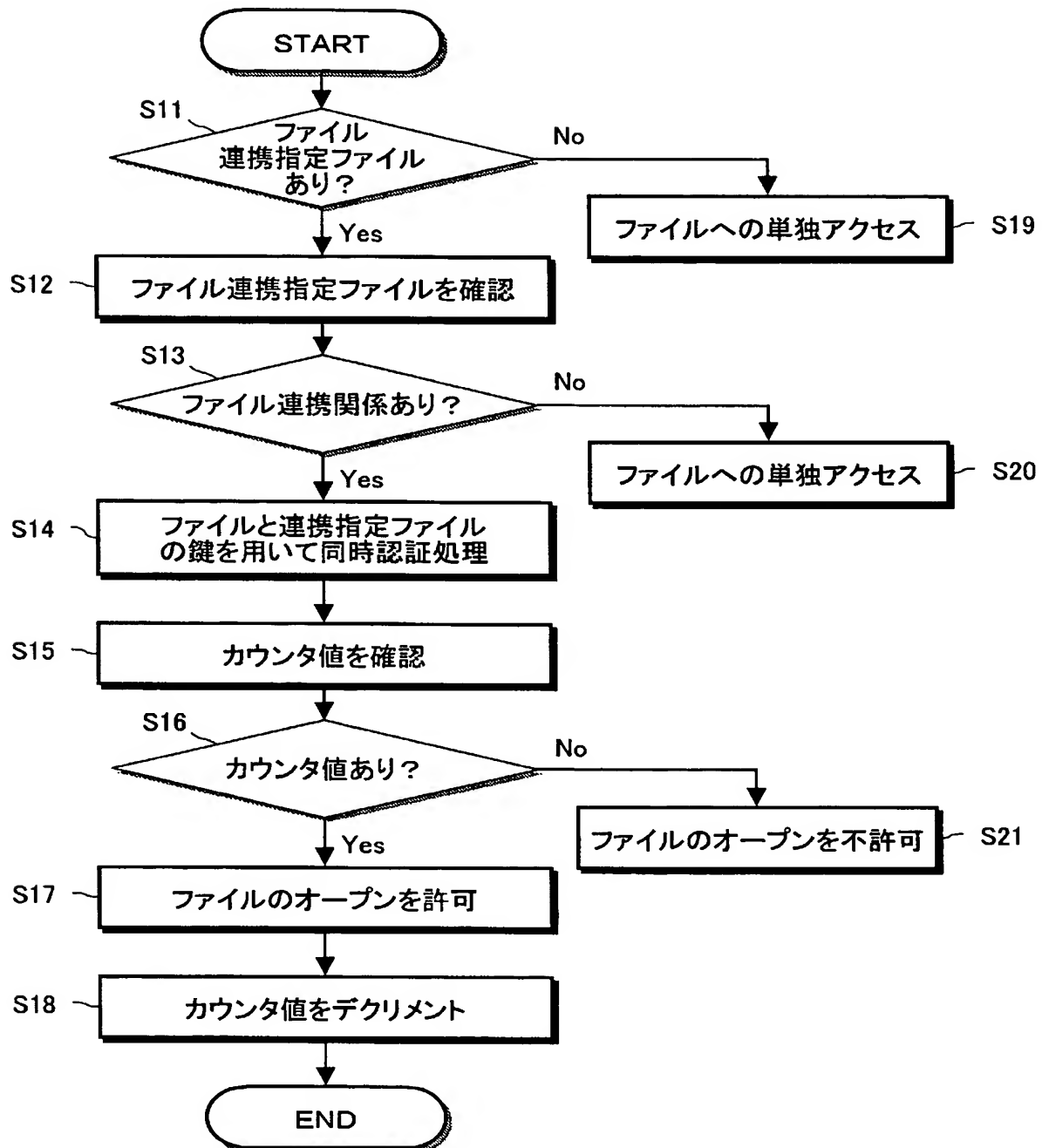
[図15]



[図16]



[図17]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2005/010599

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F12/14, 12/00, G06K17/00, 19/07, 19/073

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F12/14, 12/00, G06K17/00, 19/07, 19/073

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2005

Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2004-102465 A (Toshiba Corp.), 02 April, 2004 (02.04.04), All pages; all drawings (Family: none)	1-10
Y	JP 2003-67257 A (Sayaka ANDO), 07 March, 2003 (07.03.03), All pages; all drawings (Family: none)	1-10
Y	JP 2001-66986 A (Sony Corp.), 16 March, 2001 (16.03.01), All pages; all drawings (Family: none)	3, 4, 8, 9



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

18 August, 2005 (18.08.05)

Date of mailing of the international search report

06 September, 2005 (06.09.05)

Name and mailing address of the ISA/

Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))
Int.Cl.⁷ G06F12/14, 12/00, G06K17/00, 19/07, 19/073

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int.Cl.⁷ G06F12/14, 12/00, G06K17/00, 19/07, 19/073

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2005年
日本国実用新案登録公報	1996-2005年
日本国登録実用新案公報	1994-2005年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2004-102465 A (株式会社東芝) 2004. 04. 02, 全頁, 全図 (ファミリーなし)	1-10
Y	JP 2003-67257 A (安藤さやか) 2003. 03. 07, 全頁, 全図 (ファミリーなし)	1-10
Y	JP 2001-66986 A (ソニー株式会社) 2001. 03. 16, 全頁, 全図 (ファミリーなし)	3, 4, 8, 9

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

18. 08. 2005

国際調査報告の発送日

06. 9. 2005

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

高橋 克

電話番号 03-3581-1101 内線 3546

5 S

3044